FORTINET AND VELOCLOUD INTEGRATED SECURITY SOLUTION
Next Generation Security, Orchestration and Optimization with SD-WAN

Distributed enterprises are undergoing dramatic changes, driven by the adoption of mobility, direct Internet access, public cloud applications, and the Internet of Things (IoT). This has resulted in an exponential increase in devices, users, bandwidth, and transactions flooding their networks through the cloud applications. Modern attack surfaces are growing, the more connected and flexible enterprises become, the more opportunities it creates for cybercriminals to exploit new technologies and services that haven’t yet been fully secured.

Distributed enterprises face several challenges in deploying and managing their networks:

- **Complexity:** Deploying branch WAN edge services, configuring the WAN to access multiple destinations to increase performance and availability. Multiple paths not only increases the robustness of the infrastructure, but also results in significant increase in complexity.

- **Application Performance:** IT departments are under increasing pressure to address the constraints on bandwidth and redundancy which impact application performance and/or usage. This also increases expenses through OPEX and CAPEX.

- **Cloud Migration:** Traditional WAN architectures don’t always provide wireline-type integrity to multiple, dynamic cloud destinations, whether they be SaaS, IaaS (Infrastructure as a Service), or cloud network services.

- **Security Vulnerability:** Direct internet access by leveraging the public Internet instead of MPLS increases vulnerability of branch offices to security threats.

- **Traditional security architectures are not agile enough to support local access security, nor do they easily support zero-touch deployments to ease OPEX issues with support.**

To address the challenges of maintaining inter-site connectivity and quality of service without over-reliance on expensive circuits such as MPLS, the router or firewall responsible for WAN connectivity needs to intelligently balance internet and intranet traffic across the available WAN services. VeloCloud SD-WAN is an effective solution to this challenge, capable of providing per packet link steering at an application level and at the same time addresses needs of distributed enterprises who want to avoid deployment complexity and expensive backhaul and application performance penalties associated with conventional solutions.

Security is a key consideration in distributed deployments. Attempting to secure the modern distributed enterprise with a traditional centralized security approach is like trying to keep rain off a football game using umbrellas. What’s needed is a new distributed security architecture that mirrors and complements the new distributed enterprise – an architecture in which the entire network infrastructure is protected through a common, integral security fabric. This, in a nutshell, is the essence of Fortinet’s Distributed Enterprise Firewall (DEFW) – one of the available Deployment modes for Fortinet’s Enterprise Firewall. With Fortinet’s DFW, every remote site of the network, regardless of size, is protected under a common, scalable security fabric, the Fortinet Security Fabric. As the network expands, through new sites added to the network or through new wired or wireless connections, the fabric extends automatically, securing each new site and connection.

The Fortinet-VeloCloud Secure Software-defined WAN (SD-WAN) solution leverages Fortinet’s Distributed Enterprise Firewall (DEFW) and VeloCloud’s zero-touch deployment, one-click service insertion, single-pane management and assured application performance to provide a comprehensive, cloud-delivered secure SD-WAN solution for distributed enterprises.

**HOW DOES IT WORK?**

The Fortinet-VeloCloud Secure SD-WAN Solution consists of the Fortinet enterprise firewall platform integrated with an overlay network of VeloCloud Edges in distributed sites and data centers, as well as cloud-hosted VeloCloud Gateways and VeloCloud Orchestrator. The overlay deployment is physical transport and provider agnostic, and provides unified, automated orchestration, control and visibility, as well as business-level abstraction and incremental migration.

The solution enables distributed enterprise customers to realize the following key benefits:

- **Reduced Complexity:** VeloCloud’s end-to-end orchestration featuring zero-touch appliances provide business-level policies that enable one-click, policy-based service chaining of traffic to enterprise service hubs on the branch edge or in the cloud. Fortinet firewalls can be readily inserted in the deployment in an automated, orchestrated manner, and
the end-to-end orchestration significantly reduces complexity and deployment/operational burden and costs.

- **Increase business productivity:** VeloCloud Dynamic Multipath Optimization (DMPO) features application-aware, per-packet steering and on-demand remediation for real-time application such as voice and video, independent of the underlying transport. These capabilities ensure excellent application performance and consequent increase in business productivity.

- **Reduce Expenses:** Eliminate datacenter backhaul penalties with a cloud-ready network to provide an optimized direct path to public and private enterprise clouds. Unlike “best effort” direct branch-to-cloud alternatives, VeloCloud enables bandwidth expansion, provides direct optimal access to cloud-based applications, and enables virtual services integration in cloud and on premise while dramatically improving operational automation.

- **Enable Virtual Services:** Reduce the branch office footprint with a single click with seamless insertion and chaining of virtualized services on premise and in the cloud.

- **Unparalleled Security Protection:** Leverage the industry’s best validated security protection offered by Fortinet’s FortiGate network security platform to protect against sophisticated cyberthreats.

**USE CASES**

The following use cases highlight the value and benefits provided by the Fortinet-VeloCloud solution, enabling distributed enterprises to realize the benefits of SD-WAN in simplifying deployments and reducing costs, while doing so with unparalleled security.

**USE CASE #1: SECURE SD-WAN WITH DISTRIBUTED REGIONAL BRANCHES**

**Challenge:** Designing, implementing and maintaining service chaining and complex traffic forwarding in large, geographically distributed WAN deployments can significantly increase deployment and operational burden and costs.

**Solution:** The one-click services insertion capabilities provided by the VeloCloud business policy framework reduces complexity and aligns business policies with application needs and business objectives. The solution can eliminate hundreds of CLIs/PBR rules, resulting in reduced administrative burden. Traffic policies can be effectively managed to easily forward traffic from many branches to a selected regional data center with a VeloCloud Edge and Fortinet firewall installed.

Traffic can be readily forwarded to a regional data center for Fortinet security service insertion without the need to install additional SD-WAN hardware in the data center. The Fortinet firewall with VPN connectivity to a cloud-hosted VeloCloud Gateway can deliver connectivity to multiple branch locations, offering excellent flexibility and rapid deployment of services for IT organizations.

Fortinet's FortiGate and FortiOS have more than a hundred unique security and networking features which eliminate point products, further simplify deployments, and lower TCO (Total Cost of Ownership) along with providing the best security. Wireless and wired (switch) management, protection, and guest-networking can often be the next steps in a process for deploying a remote site office. The provisioning of ports and wireless access can be a cumbersome and expensive task. The Fortinet FortiGate wireless AP and switch controller provides a controller to ease AP deployment and take complexity and security concerns out of deploying ports for phones and user data.

Fortinet provides physical and logical topology visualization and other powerful capabilities in FortiOS’s FortiView, which leverages the Fortinet Security Fabric functionality to allow greater visibility, oversight and control of the network. The Security Fabric enables network and security components to collect and share information in order to coordinate and effectively respond to security threats. As illustrated in the figure, these powerful features provide unparalleled network security visibility and control.
USE CASE #2: SECURE OPTIMIZED ACCESS TO IAAS SERVICES

Challenge: With enterprises increasingly leveraging cloud services to run their data center workloads, IT departments often run into challenges of increased complexity as a result of having to manually configure “NxN” secure overlay tunnels to access their “N” VPC instances from “N” branches. They also lose performance and security when doing so.

Solution: VeloCloud Gateways at the enterprise branches automatically set up a secure and optimized overlay using VeloCloud Dynamic Multipath Optimization. The VeloCloud Gateway service chains the VPC instances, thereby requiring only N tunnels, avoiding the complexity associated with creating NxN tunnels in a traditional scenario, and ensures optimization for application performance. Fortinet FortiGate-VM for AWS (Amazon Web Services) can be deployed on-demand, thereby ensuring enterprise-grade security by having FortiGate firewalls and FortiWeb Web Application Firewalls in the IaaS environment. This delivers a high level of automation and curated threat intelligence directly to cloud applications that might suffer attacks directly from the platform they are delivered on.

USE CASE #3: SECURITY WITH VIRTUAL CPE

Challenge: Organizations are increasingly pressured to reduce costs and eliminate the administrative complexity, truck rolls and burden associated with deploying and managing CPE equipment and physical appliances at branch sites.

Solution: Organizations can deploy the VeloCloud Gateway together with Fortinet FortiGate-VM VNF, thereby reducing management burden and costs. Alternatively, they can deploy the Fortinet FortiGate-VM VNF on the VeloCloud Edge for ease in enabling distributed firewall services and wired and wireless control to deliver secure access for employees, guests, and contractors for the enterprise.

USE CASE #4: SERVICE PROVIDER DEPLOYMENTS

Challenge: The rise in online collaboration and rich media applications is driving enterprises to explore using Internet links for economical expansion of their private MPLS networks. To satisfy these requirements, service providers need a solution to augment existing network services effectively. Both enterprises and their service providers must adapt their network architecture to accommodate the increasing shift of applications and datacenters to the cloud while delivering the expected levels of reliability, performance, and security. Service providers are challenged to evolve, adapt and expand their service offerings to meet customers’ needs, and are in need of solutions to offer advanced SD-WAN services to their customers.

Solution: Service providers can leverage the solution to deploy Fortinet firewalls and VeloCloud multi-tenant gateways as VNFs in their cloud environment, thereby delivering both “last mile” optimized performance to remote cloud and centralized enterprise services. In addition, service providers can offer unparalleled security by leveraging the industry’s best validated security protection offered by Fortinet’s FortiGate network security platform. Service providers are increasingly seeking to increase their portfolio for services in the field. Customers are looking to offload headaches that are hard to automate and deliver, such as wireless and wired (switch) management, protection, and guest-networking, which can often be the next steps in a process for deploying a remote site office. The provisioning of ports and wireless access can be a cumbersome and expensive task.
The Fortinet FortiGate, wireless AP and switch controller ease AP deployment and take complexity and security concerns out of deploying ports for phones and user data, while providing protection against sophisticated cyberthreats.

**ABOUT VELOCLOUD**

VeloCloud, a Cloud-Delivered SD-WAN pioneer simplifies branch WAN networking by automating deployment and improving performance over private, broadband Internet and LTE links for today’s increasingly distributed enterprises, as well as service providers.

Learn more at [http://www.velocloud.com/](http://www.velocloud.com/)